DEPARTMENT OF COMMERCE

National Technical Information Service

15 CFR Part 1110

[Docket Number: 160511004-4999-04]

RIN 0692-AA21

Certification Program for Access to the Death Master File

AGENCY: National Technical Information Service, U.S. Department of Commerce.

ACTION: Final rule.

SUMMARY: The National Technical Information Service (NTIS) issues this final rule establishing a program through which persons may become eligible to obtain access to Death Master File (DMF) information about an individual within three years of that individual's death. This final rule supersedes and replaces the interim final rule that NTIS promulgated following passage of Section 203 of the Bipartisan Budget Act of 2013 to provide immediate and ongoing access to persons who qualified for temporary certification. The program established under this final rule contains some changes from the proposed rule published by NTIS.

DATES: This final rule is effective [INSERT DATE 180 DAYS FROM DATE OF PUBLICATION IN FEDERAL REGISTER].

FOR FURTHER INFORMATION CONTACT: Brian Lieberman, Senior Counsel for NTIS, at blieberman@ntis.gov, or by telephone at 703-605-6404. Information about the DMF made available to the public by NTIS may be found at https://dmf.ntis.gov.

SUPPLEMENTARY INFORMATION:

Background:

This final rule is promulgated under Section 203 of the Bipartisan Budget Act of 2013, Pub. L. 113-67 (Act), passed into law on December 26, 2013. The Act prohibits the Secretary of Commerce (Secretary) from disclosing DMF information during the three-calendar-year period following an individual's death (referred to as the "Limited Access DMF," or "LADMF"), unless the person requesting the information has been certified to access that information pursuant to certain criteria in a program that the Secretary establishes. The Act further requires the Secretary to establish a fee-based program to certify Persons for access to LADMF. In addition, it provides for penalties for Persons who receive or distribute LADMF without being certified or otherwise satisfying the requirements of the Act. The Secretary has delegated the authority to carry out Section 203 to the Director of NTIS.

The Act mandated that no person could receive LADMF without certification after March 26, 2014 (i.e., 90 days from enactment of the Act). NTIS acted promptly to ensure that a suitable certification program was in place by that date, and to avoid interruption of access by legitimate users of the data. On March 3, 2014, NTIS published a Request for Information (RFI) and Advance Notice of Public Meeting on the Certification Program for Access to the Death Master File (79 FR 11735). NTIS held the public meeting, with webcast, on March 4, 2014. Written comments received in response to the RFI, and a transcription of oral comments submitted at the public meeting, may be viewed at https://dmf.nist.gov.

On March 26, 2014, NTIS published an interim final rule, "Temporary Certification Program for Access to the Death Master File" (interim final rule) (79 FR 16668). That rule codified an interim approach to implementing the Act's provisions pertaining to the certification program and the penalties for violating the Act, and set out an interim fee schedule for the program. NTIS published the interim final rule in order to provide a mechanism for Persons to access LADMF immediately on the effective date

prescribed in the Act. Written comments received in response to the Interim Final Rule may be viewed at http://www.regulations.gov.

The preambles for both the RFI and the interim final rule set out the specific provisions of the Act, and also noted that several Members of Congress described their understanding of the purpose and meaning of Section 203 during Congressional debate on the Joint Resolution which became the Act. Citations to those Member statements were provided in the RFI, which also provided background on the component of the DMF, which originates from the Social Security Administration, covered by Section 203. The interim final rule was established to provide immediate access to the LADMF to those users who demonstrated a legitimate fraud prevention interest, or a legitimate business purpose for the information, and to otherwise delay the release of the LADMF to all other users, thereby reducing opportunities for identity theft and restricting information sources used to file fraudulent tax returns.

In addition, in December, 2014, NTIS issued an initial public draft of "Limited Access Death Master File (Limited Access DMF) Certification Program Publication 100," (Publication 100), available at https://dmf.ntis.gov. Publication 100 is the NTIS security guideline document for persons certified under this final rule. Publication 100 sets forth suggested security controls, standards and protocols for the protection of LADMF in the possession of Certified Persons.

On December 30, 2014, NTIS published the proposed rule (79 FR 78314). The proposed rule introduced changes, clarifications and additions to the interim final rule, based in part upon comments received. For example, the proposed rule introduced a "safe harbor" provision, § 1110.103, which would exempt a Certified Person from penalty for disclosure of LADMF to another Certified Person. The proposed rule set forth a provision for review, assessment, audit and attestation of a Person's information and information security controls by independent, third party conformity assessment bodies. Section 1110.201 of the proposed rule would permit Certified Persons to provide the attestation of an

"Accredited Certification Body" (as defined in § 1110.2) concerning the adequacy of the Certified Person's "systems, facilities and procedures in place to safeguard DMF information."

NTIS requested that all written comments on the proposed rule be submitted to Regulations.gov by January 31, 2015. The agency, however, received requests to extend the public comment period. In response, on January 28, 2015, NTIS published a notice extending the comment period until March 30, 2015 (80 FR 4519). Written comments received in response to the proposed rule may be viewed at http://www.regulations.gov.

Comments in Response to the Proposed Rule

In response to the proposed rule, NTIS received 62 written comments. The commenters included one foreign government, twenty industry and trade associations, five service providers, three financial services companies, two insurance companies, four health care and medical research organizations and five service providers. The remainder of the commenters were primarily individuals, including a number identifying themselves as genealogists.

In preparing this final rule, NTIS has carefully considered all comments received in response to the proposed rule. Many commenters requested that NTIS provide unrestricted access to LADMF. However, NTIS cannot revise the rule to accommodate such comments, since access to and use of LADMF is governed by the statutory provisions set forth in Section 203 of the Act. A number of commenters requested changes to the composition of the DMF itself; however, the composition of the DMF is explicitly defined in Section 203(d) of the Act as consisting of "the name, social security account number, date of birth and date of death of deceased individuals maintained by the Commissioner of Social Security." NTIS, therefore, has no discretion to alter the composition of the DMF. Some commenters suggested that NTIS should enhance search capabilities available to DMF subscribers. NTIS has no present plans to alter database search capabilities, but may consider doing so in the future. However,

NTIS's database search capabilities are not an element of this final rule. NTIS also received multiple comments to the effect that the proposed subscription cost of the LADMF should be reduced; however, Section 203(b)(3) mandates the charge of fees sufficient to cover costs associated with the certification program. The certification fee that NTIS charges covers the costs of receiving and processing applications, including authenticating the statements made in the application, and ensuring access to the Limited Access DMF.

A number of comments were received asserting that some Certified Persons need to provide LADMF date of death information in the ordinary course of their business, for example, to retirement plans and others who have a legal obligation to provide death benefits payments to beneficiaries or for other legitimate purposes, and some suggested that the rule should specifically provide for the disclosure of date of death information alone as an exception to requirement for certification. However, as noted above, "date of death" is one of the four elements (the others being name, social security number, and date of birth) expressly set forth in the statutory definition of the term "Death Master File" under the Act, and NTIS is without discretion to categorically exclude it through rulemaking. NTIS notes that it received no comments suggesting that retirement plans and others having a legal obligation to provide death benefits would be unable to demonstrate one or more of a legitimate fraud prevention interest, business purpose, or fiduciary duty, to qualify for certification or, if not certified, that they would be unable to demonstrate, first, that they meet the requirements for LADMF access (i.e., the legitimate fraud prevention or business purpose and security requirements of § 1110.102(a)(1), (2), and (3)), and, second, that they would not misuse or further disclose LADMF to a person who would either wrongfully use LADMF or could not comply with the security requirements set forth in § 1110.200(a)(1)(ii) or (iii) respectively. NTIS points out that "fact of death," i.e., the fact that a person is no longer living, confirmation of which was identified by some commenters as important for legitimate business

purposes, is not an element of the statutory definition of the term “Death Master File,” and will not be considered by NTIS to be equivalent to “date of death” under the final rule.

NTIS also notes that the proposed rule would revise the definition of “Limited Access DMF” to provide that an individual element of information (name, social security number, date of birth, or date of death) in the possession of a Person, whether or not certified, but obtained by such Person through a source independent of the Limited Access DMF, would not be considered “DMF information.” That revision is retained in the final rule, and has been further clarified in response to comments. Specifically, NTIS has replaced the term “Certified Person” in the last sentence of the LADMF definition with “Person” to make clear that any Person, whether or not certified, who obtains an individual element of information independently is not considered to possess “Limited Access DMF.”

Comments were received suggesting that, for clarity and simplicity, the final rule should refer to the defined term “Limited Access DMF” to the extent possible. NTIS has incorporated these comments into the final rule, including §§ 1110.102(a)(4) and 1110.200(a)(1).

NTIS received comments supporting the provision of the proposed rule that would amend § 1110.102(a)(2) and (3) to clarify that, to be certified to obtain access to the Limited Access DMF, a Person must certify both that the Person has systems, facilities, and procedures in place to safeguard the accessed information, and experience in maintaining the confidentiality, security, and appropriate use of accessed information, pursuant to requirements similar to the requirements of section 6103(p)(4) of the Internal Revenue Code of 1986, and that the Person “agrees to satisfy such similar requirements.” This standard differs from the requirement of Section 203 of the Act, because that Section contains contradictory statements about the types of systems to safeguard information that a Certified Person must have in place. In Section 203(b)(2)(B), the Act states that in order to receive Limited Access DMF, a Person must agree to comply with requirements “similar to” Section 6103(p)(4) of the Internal Revenue

Code (IRC). Section 6103(p)(4) of the IRC is directed to Federal government agencies, and as such the "similar to" statement makes sense for non-government actors which are the subject of the Act. However, Section 203(b)(2)(C) requires a Certified Person to also "satisfy the requirements of such section 6103(p)(4) as if such section applied to such person." It is unclear how or why a Certified Person could or should satisfy safeguarding requirements "similar to" section 6103(p)(4) of the IRC, while also satisfying section 6103(p)(4) of the IRC. In addition, commenters pointed out that some of the provisions of section 6103(p)(4) could not reasonably be imposed on non-government actors, because, for example, in contrast to Federal Tax Information, Limited Access DMF under Section 203 is not subject to restriction when beyond the three-calendar-year period following the date of death.

To resolve this ambiguity and address these comments, NTIS interprets Section 203(b) of the Act as requiring Persons to certify that they have systems, facilities, and procedures in place that are "reasonably similar to" those required by section 6103(p)(4) of the IRC in order to become Certified Persons. This interpretation allows NTIS to meet the interest of protecting personal data generally and deterring fraud, while also allowing NTIS to set the data integrity standards appropriate to safeguard Limited Access DMF specifically. The final rule amends § 1110.102(a)(2) and (3) accordingly.

A number of commenters suggested that the final rule should expressly classify certain categories of activities or enterprises, such as health care research and insurance investigation, as "a legitimate fraud prevention interest" or "a legitimate business purpose." Other commenters suggested that the final rule should specifically provide that when an applicant or Certified Person is subject to other laws governing the use of personal information, the applicant or Certified Person should for that reason be deemed to have a "legitimate fraud prevention interest" or "legitimate business purpose." It was urged that codification of such categories would further the purpose of the Act and benefit businesses and other entities reliant upon the LADMF by eliminating the threat of interrupted access. NTIS has carefully

considered these suggestions, and observes that each Person applying for certification must certify to NTIS that such Person satisfies each of three requirements specified under Section 203(b)(2) of the Act, and that NTIS will evaluate each application individually to ensure that an individual applicant is properly certified. NTIS does acknowledge that it received numerous comments to the effect that awardees of federal research grants and others conducting extramural and intramural research under federal programs should be eligible for certification, provided that they otherwise satisfy the requirements of the final rule. NTIS notes that, while it appreciates the commenters' position, such Persons must, like any applicants, demonstrate that they satisfy the requirements for LADMF access.

A commenter observed that use of the term "Accredited Certification Body" in the proposed rule could create confusion, particularly since the concept of "certification" appears and is used separately in the rule. Accordingly, the final rule uses the term "Accredited Conformity Assessment Body" rather than "Accredited Certification Body," and NTIS uses the former term in the preamble as well.

A number of commenters urged that particular activities and enterprises, such as direct marketing and life insurance companies, should not be subject to DMF-related audits or required to obtain a written third party attestation, where such activities and enterprises are independently subject to regulatory scrutiny and must comply with the privacy security requirements of other laws, such as the Gramm-Leach-Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA), and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). While NTIS will decline to exclude Persons from the requirement for attestation as part of the certification process under the final rule, and will decline to exclude Certified Persons from being subject to audit, NTIS emphasizes that it is NTIS's intent under this final rule that applicants and Certified Persons should not incur the burden or expense of a DMF-specific audit when they have already had, or will have, an appropriate independent assessment or audit performed for other purposes, including but not limited to those noted above. To this end, § 1110.503(c) of the final

rule explicitly contemplates reliance upon a review or assessment or audit by an Accredited Conformity Assessment Body that was not conducted specifically or solely for the purpose of submission to NTIS. NTIS intends that when a review, assessment or audit has been or can be performed in the course of satisfying other Federal, state, tribal, or local government laws or regulations, such as those mentioned by commenters, or other regulatory or fiduciary requirements flowing from such laws or regulations, a Person or Certified Person will be able to rely upon that review, assessment or audit, to the extent that the requirements of the final rule are satisfied. In these circumstances, NTIS intends that it will accept an Accredited Conformity Assessment Body's attestation regarding a non-DMF audit, which attestation includes an explanation of the nature of that non-DMF audit and represents that, based on its review, the Accredited Conformity Assessment Body is satisfied that the LADMF security and safeguard requirements are met.

NTIS will not at this time accept the suggestion of some commenters to permit "self-assessments" or "a self-certified written attestation" in lieu of a written attestation from an independent Accredited Conformity Assessment Body. With respect to state and local government departments and agencies, which are included within the definition of Persons in the final rule, NTIS notes some commenters' concerns that the proposed rule could burden such departments and agencies given state-established information security and safeguarding procedures, and agrees with the recommendation of a commenter that it should accept written attestation from an independent state or local government Inspector General or Auditor General office.

Accordingly, provided that a state or local government Inspector General or Auditor General satisfies the requirements of the final rule for Accredited Conformity Assessment Bodies, new § 1110.501(a)(2) of the final rule provides that a state or local government office of Inspector General or Auditor General and a Person or Certified Person that is a department or agency of the same state or local government,

respectively, are not considered to be owned by a common "parent" entity under § 1110.501(a)(1)(ii) for the purpose of determining independence, and attestation by the Inspector General or Auditor General will be possible.

With respect to comments urging that provision should be made for self-assessments and attestations by organizations having the capacity to perform assessments and audits, NTIS recognizes that some organizations have such capacity, and are able in exercising it to address safeguarding and security requirements under other laws and regulations. Accordingly, new § 1110.502 of the final rule provides that, in addition to "independent" Accredited Conformity Assessment Bodies, a Person or Certified Person may engage a "firewalled" Accredited Conformity Assessment Body, as defined in the final rule and with the approval of NTIS, under conditions, as defined in the rule, which ensure that concerns about independence and actual or apparent conflicts of interest or undue influence are satisfactorily addressed.

Under new § 1110.502(a), a third party conformity assessment body must apply to NTIS for firewalled status if it is owned, managed, or controlled by a Person or Certified Person that is the subject of attestation or audit by the Accredited Conformity Assessment Body, applying the characteristics set forth under § 1110.501(a)(1) for independence. Under new § 1110.502(b), NTIS will accept an application for firewalled status when it finds that: (1) acceptance of the third party conformity assessment body for firewalled status would provide equal or greater assurance that the Person or Certified Person has information security systems, facilities, and procedures in place to protect the security of the Limited Access DMF than would the Person's or Certified Person's use of an independent third party third party conformity assessment body; and (2) the third party conformity assessment body has established procedures to ensure that: (1) its attestations and audits are protected from undue influence by the Person or Certified Person that is the subject of attestation or audit by the Accredited

Conformity Assessment Body, or by any other interested party; (2) NTIS is notified promptly of any attempt by the Person or Certified Person that is the subject of attestation or audit by the third party conformity assessment body, or by any other interested party, to hide or exert undue influence over an attestation, assessment or audit; and (3) allegations of undue influence may be reported confidentially to NTIS. To the extent permitted by Federal law, NTIS will undertake to protect the confidentiality of witnesses reporting allegations of undue influence. Under new § 1110.502(c), NTIS will review each application and may contact the third party conformity assessment body with questions or to request submission of missing information, and will communicate its decision on each application in writing to the applicant.

Some commenters expressed concern that in attesting to its credentials under § 1110.503(a), an Accredited Conformity Assessment Body must indicate that it is accredited to a nationally or internationally recognized standard such as the ISO/IEC Standard 27006-2011 or any other similar recognized standard for bodies providing audit and certification for information security management systems, pointing to other potentially applicable standards, such as the American Institute of Public Accountants (AICPA) Service Organization Control Report (SOC) Type 2 Audit Report. NTIS wishes to emphasize that it is not NTIS's intent, in reciting ISO/IEC 27006-2011, to exclude from consideration AICPA SOC2 or other appropriate accreditation standards. The regulation identifies the ISO/IEC standard as one example of an acceptable national or international accreditation standard. NTIS selected the ISO/IEC standard, as noted in the original discussion of the proposed rule, to serve "as a baseline for accreditation," because it was prepared by the International Organization for Standardization (ISO) Committee on conformity assessment (79 FR at 78316). Moreover, NTIS emphasized that it is "is aware that standards other than ISO/IEC 27006-2001 exist that may be equally appropriate for the purposes of accreditation under the Act, and that additional standards may be developed in the future … an [Accredited Conformity Assessment Body] may attest, subject to the conditions of verification in [final

rule] Section 1110.503, that it is accredited to a nationally or internationally recognized standard for management systems other than ISO/IEC Standard 27006-2011." NTIS further observes that the burden rests with the Person or Certified Person to identify and submit an attestation by an Accredited Conformity Assessment Body certified or credentialed by an appropriate accrediting body. Accordingly, NTIS concludes that § 1110.503(a) provides appropriate guidance as to the accreditation standard for Accredited Conformity Assessment Bodies.

A few commenters suggested that NTIS should directly accredit Accredited Conformity Assessment Bodies to conduct assessments and audits or provide a list of acceptable accreditations for Accredited Conformity Assessment Bodies. NTIS does not intend to do so. Recognized professional accreditation organizations with well-established, rigorous accreditation processes already exist in the private sector. Such organizations have either adopted or established nationally and internationally accepted standards for entities which may serve as Accredited Conformity Assessment Bodies under the final rule. In considering how to establish a permanent certification program as required under Section 203, NTIS carefully considered developing, within the agency, the capacity to evaluate the information systems, facilities and procedures of Persons to safeguard Limited Access DMF, as well as to conduct audits of Certified Persons and to itself accredit conformity assessment bodies. NTIS has consulted with the National Institute of Standards and Technology (NIST), which has expertise in testing, standard setting, certification and conformity assessment. Based on NIST recommendations, NTIS believes it appropriate for private sector, third party, Accredited Conformity Assessment Bodies to attest to a Person's information security safeguards under § 1110.102(a)(2) of the rule, for NTIS to rely upon such attestation in certifying a Person under the final rule, and for NTIS to rely as well upon third party, private sector accreditation of Accredited Conformity Assessment Bodies, while reserving to itself the ability to perform assessments and audits itself, in its discretion.

A number of commenters expressed concerns regarding the identification, in § 1110.502(b) of the proposed rule, of the "Limited Access Death Master File Publication 100" (Publication 100) as a source of guidance to which an Accredited Conformity Assessment Body could refer in its attestation as to the adequacy of an applicant's or Certified Person's safeguards for Limited Access DMF. These commenters stated that, even though Publication 100 is intended to set forth recommended guidelines, procedures and best practices, reference to that publication in the proposed rule implied a limitation to those safeguarding approaches set forth in Publication 100. These commenters offered other sources of security requirements for personal information they thought were pertinent and should be expressly included in the rule, such as the security standards for the GLBA.

NTIS notes, however, that the language of the rule makes clear that Publication 100 merely offers an example of security controls and protocols that an applicant or Certified Person may use, and is not intended to be prescriptive (79 FR at 78316). Moreover, NTIS recognizes that "a number of different approaches exist to safeguarding information." Id. In the December 2014 Draft Version of Publication 100, NTIS stated:

> "These information security guidelines are derived from NIST SP800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. Only NIST SP 800-53 controls believed to be essential to the protection of Limited Access DMF information are included in this publication as a baseline. Applicability was determined by selecting controls relevant to protecting the confidentiality of Limited Access DMF information. The NIST controls [discussed here] are intended by NTIS to be illustrative, not exclusive. Other controls that can be assessed and used as guidelines include the NIST Framework for Improving Critical Infrastructure Cybersecurity v1.0. The Framework Core provides a common set of activities for managing risks, and associated controls. The references provided in the Framework Core

represent a diverse set of information security guidelines including: International Organization for Standardization ISO 27001; International Society for Automation ISA/IEC 62443; Control Objectives for Information and Related Technology COBIT; Council on Cybersecurity Critical Security Controls CCS CSC2; and NIST 800-53 rev. 4. Again, these references are illustrative."

Nevertheless, in response to commenters' concerns, NTIS has removed reference to Publication 100 from § 1110.503(b) of the final rule. Given the continuously evolving nature of information technology security and safeguard guidelines, procedures and best practices, NTIS intends that Publication 100 will be a living document. NTIS has invited comments on Publication 100 from the public on an ongoing basis, and contemplates interactive public dialog regarding its contents.

The proposed rule introduced a "safe harbor" provision in § 1110.200(c) that would exempt from penalty a first Certified Person who discloses LADMF to a second Certified Person, where the first Certified Person's liability rests solely on the fact that the second Certified Person has been determined to be subject to penalty. The provision was specifically drafted to apply to each disclosure and to limit the presumption of compliance to the first Certified Person, while the second Certified Person (i.e., the recipient of the LADMF) remained subject to penalty for violations of the Act (79 FR at 78317.) NTIS invited comments as to whether the "safe harbor" provision should be extended to circumstances where the recipient is believed to be certified but, in fact, is not. NTIS did not receive comment on this point. A Certified Person desiring to rely upon the "safe harbor" provision as set forth in this final rule will bear responsibility for ensuring that a recipient of LADMF is, in fact, a Certified Person at the time of disclosure. NTIS notes that it maintains and publishes a list of Certified Persons, available at https://dmf.ntis.gov.

NTIS received many comments suggesting that it should promulgate a broader "safe harbor" for a Certified Person who discloses LADMF to Persons whom the Certified Person knows are not certified

("uncertified Persons"). Many commenters urged that, unless the final rule made further allowance for Certified Persons to share LADMF with uncertified Persons, the commenters' businesses would suffer and their clients or other users would be deprived of data they need for critical purposes including fraud prevention, record-keeping and meeting legal and regulatory obligations. Many of these commenters also urged the extension of the "safe harbor" to Certified and uncertified Persons under certain circumstances, such as where an uncertified Person attests in writing that it meets the requirements for certification and to disclose the LADMF only to other uncertified Persons who could also meet the requirements, or where private contractual obligations were incurred. Some commenters contended that it would be unreasonable and unrealistic for NTIS to require their clients or other users to become certified and thus be subject to the rule's security and auditing requirements.

NTIS will not extend the "safe harbor" provision of § 1110.102(c) in this manner. However, NTIS emphasizes that Certified Person status has not been and is not required in order for a Certified Person to disclose LADMF to another Person. A Certified Person may, without penalty under § 1110.200 (but without "safe harbor" protection), disclose LADMF to another Person who, although not certified, meets the requirements of § 1110.102(a)(1) through (3), and who does not misuse or further disclose the LADMF in violation of § 1110.200(a)(1)(ii) or (iii). Indeed, many of the comments described above reflect the types of procedures that Certified Persons have successfully adopted under the Temporary Certification Program, and might be expected to adopt successfully in disclosing LADMF to uncertified Persons under the final rule. However, under such circumstances not involving a certified recipient, NTIS will not apply a "safe harbor" such as is applied under the final rule to a Certified Person who discloses Limited Access DMF to another who is also a Certified Person.

A few commenters were critical of the appeals process set forth in §1110.300. One commenter opined that entities facing potential liability through "unscheduled audits" and "substantial financial penalties"

needed “well-developed procedural rights” such as the right of appeal to an administrative law judge and federal court. NTIS has carefully considered these comments, but concludes that the process and procedures set forth in §1110.300 are legally sufficient. NTIS has provided an appropriate administrative and appeal process in §1110.300. Pursuant to the Administrative Procedure Act (Pub. L. 79–404, 60 Stat. 237), any Person or Certified Person can seek review of any adverse action or decision by the Director of NTIS in federal district court.

A comment was received suggesting that the exclusion of Executive departments or agencies of the United States Government from the definition of “Persons,” noted initially under the interim final rule and continued in the proposed rule, should be extended as well to the governments of foreign countries. NTIS has carefully considered this comment, but will not adopt such a categorical exclusion. NTIS will continue to consider applications by foreign governments on a case-by-case basis, in accordance with general principles of comity and consistent with the purposes of Section 203 and the requirements of the final rule.

The Final Rule

This final rule amends subparts A, B, C, D, and adds a new subpart E to the DMF Certification Program in part 1110 of title 15 of the Code of Federal Regulations. The following describes specific provisions being amended.

Under § 1110.2, “Definitions,” NTIS is revising the definition of “Person” to recite “state and local government departments and agencies,” so that “Person” will be defined as including corporations,

companies, associations, firms, partnerships, societies, joint stock companies, and other private organizations, and state and local government departments and agencies, as well as individuals. However, Executive departments or agencies of the United States Government will not be considered "Persons" for the purposes of this rule. Accordingly, Executive departments or agencies will not have to complete the Certification Form as set forth in the rule, and will be able to access Limited Access DMF under a subscription or license agreement with NTIS, describing the purpose(s) for which Limited Access DMF is collected, used, maintained and shared. Those working on behalf of and authorized by Executive departments or agencies may access the Limited Access DMF from their sponsoring Executive department or agency, which will be responsible for ensuring that such access is solely for the authorized purposes described by the agency. Unauthorized secondary use of Limited Access DMF by Executive departments or agencies or those working for them or on their behalf is prohibited. If an Executive department or agency wishes those working on its behalf to access the Limited Access DMF directly from NTIS, then those working on behalf of that Executive department or agency will be required to complete and submit the Certification Form as set forth in the rule and enter into a subscription agreement with NTIS in order to directly access the Limited Access DMF. Under this final rule, a Certified Person will be eligible to access the Limited Access DMF made available by NTIS through subscription or license.

The final rule adds a requirement that, in order to become certified, a Person must submit a written attestation from an Accredited Conformity Assessment Body, as defined in the final rule, that such Person has information security systems, facilities, and procedures in place to protect the security of the Limited Access DMF, as required under § 1110.102(a)(2) of the rule. NTIS has consulted with NIST, which has expertise in testing, standard-setting, and certification of various systems. Based on NIST recommendations, the final rule provides for private sector, third party, Accredited Conformity Assessment Bodies to attest to a Person's information security safeguards under § 1110.102(a)(2) of the

rule, and NTIS will rely upon such attestation in certifying a Person under the final rule. The final rule also provides for Accredited Conformity Assessment Bodies to conduct periodic scheduled and unscheduled audits of Certified Persons on behalf of NTIS.

Under the final rule, an "Accredited Conformity Assessment Body" is defined as an independent third party conformity assessment body that is not owned, managed, or controlled by a Person or Certified Person which is the subject of attestation or audit, and that is accredited by an accreditation body under nationally or internationally recognized criteria such as, but not limited to, ISO and the International Electrotechnical Commission (IEC) publication ISO/IEC 27006-2011, "Information technology—Security techniques—Requirements for bodies providing audit and certification of information security management systems," to attest that a Person or Certified Person has information technology systems, facilities and procedures in place to safeguard Limited Access DMF. Based on NIST recommendations, NTIS believes it is appropriate to reference the ISO/IEC 27006-2001 as an exemplary baseline for accreditation under the final certification program. The ISO Committee on conformity assessment (CASCO) prepared ISO/IEC 27006-2001, and reference to the ISO/IEC standard will help ensure that attestations and audits under the final certification program operate in a manner consistent with national and international practices. Accreditation is a third-party attestation that a conformity assessment body operates in accordance with national and international standards. Accreditation is used nationally and internationally in many sectors where there is a need, through certification, for safety, health or security requirements to be met by products or services. Accreditation ensures that a conformity assessment body is technically competent in the subject matter (in this case, the information safeguarding and security requirements as set forth in the rule) and has a management system in place to ensure competency and acceptable certification program operations on a continuing basis. Accreditation requires that Accredited Conformity Assessment Bodies be re-accredited on a periodic basis.

However, NTIS also acknowledges that standards other than ISO/IEC 27006-2001 exist that are equally appropriate for the purposes of accreditation under the Act, and that additional appropriate standards may be developed in the future. The final rule provides that an Accredited Conformity Assessment Body may attest, subject to the conditions of verification in § 1110.503 of the final rule, that it is accredited to a nationally or internationally recognized standard for bodies providing audit and certification of information security management systems other than ISO/IEC Standard 27006-2011. In addition, the rule provides that an Accredited Conformity Assessment Body must also attest that the scope of its accreditation encompasses the information safeguarding and security requirements as set forth in the rule.

NTIS is aware that security and safeguarding of information and information systems is of great concern in many fields of endeavor other than with respect to Limited Access DMF. NTIS has consulted with subject matter experts from NIST, which in 2014 published the "Framework for Improving Critical Infrastructure Cybersecurity"[1] (Framework), in response to President Obama's Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," which established that "[i]t is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." In articulating this policy, the Executive Order calls for the development of a voluntary risk-based Cybersecurity Framework—a set of industry standards and best practices to help organizations manage cybersecurity risks. The resulting Framework, created by NIST through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risks in a cost-effective way based on business needs without placing additional regulatory requirements on businesses. The Framework enables

[1] This document can be found at: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

organizations—regardless of size, degree of cybersecurity risk, or cybersecurity sophistication—to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. The Framework provides organization and structure to today's multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today. Accordingly, in addressing the requirements of Section 203 for "systems, facilities, and procedures" to safeguard Limited Access DMF, NTIS contemplates that Persons, as well as Accredited Conformity Assessment Bodies, may look to the Framework and to the Framework's Informative References. The Framework is referenced by NTIS in Publication 100. As set forth in Publication 100, as well as in the Framework's Informative References, a number of different approaches exist to safeguarding information. These include ISO/IEC, Control Objectives for Information and Related Technology (COBIT), International Society of Automation (ISA), and NIST's 800 series publications. Others include the Service Organization Controls (SOC) of the American Institute of CPAs (AICPA).

NTIS is aware that security and safeguarding assessments such as those contemplated under this final rule are routinely carried out in the private sector, including by entities which may satisfy the requirements for Accredited Conformity Assessment Bodies under the rule. Provided that such a routine assessment or audit of a Person would permit an Accredited Conformity Assessment Body to attest that such Person has systems, facilities, and procedures in place to safeguard Limited Access DMF as required under § 1110.102(a)(2) of the final rule, albeit carried out for a purpose other than certification under the rule, NTIS will accept an attestation in support of a Person's certification with respect to the requirements under § 1110.102(a)(2) of the rule, as well as in support of the renewal of a Certified Person's certification. The final rule provides that any attestation, whether for a Person seeking certification or for a Certified Person seeking renewal, must be based on the Accredited Conformity Assessment Body's review or assessment conducted no more than three years prior to the date of submission of the Person's completed certification statement or of the Certified Person's completed

renewal certification statement. As noted, an Accredited Conformity Assessment Body's review or assessment need not have been conducted specifically or solely for the purpose of submission of an attestation under the final rule. From NTIS's consultations with NIST subject matter experts, NTIS believes that the limitation of three years is appropriate as to frequency for assessments for the security and safeguarding of information and information systems, and that permitting Persons and Certified Persons to rely on attestations based on such assessments conducted for purposes other than solely for the rule is reasonable and cost-effective.

Persons previously certified under the interim final rule will need to become certified in accordance with the requirements of this final rule, when it becomes effective. Certification under this final rule will include an updated certification form (NTIS FM161), discussed under the heading, “Paperwork Reduction Act,” collecting additional information that will improve NTIS's ability to determine whether a Person meets, to the satisfaction of NTIS, the requirements of Section 203 of the Act.

Under § 1110.103 of the final rule, a Certified Person may disclose Limited Access DMF to another Certified Person, and will be deemed to satisfy the disclosing Certified Person's obligation to ensure compliance with final § 1110.102(a)(4)(i)-(iii) for the purposes of certification. Similarly, under § 1110.200(c), NTIS will not impose a penalty, under § 1110.200(a)(1)(i)-(iii) of the final rule, on a first Certified Person who discloses Limited Access DMF to a second Certified Person, where the first Certified Person's liability rests solely on the fact that the second Certified Person has been determined to be subject to penalty. While the final rule does not restrict disclosure of Limited Access DMF to Certified Persons, these provisions create an appropriately limited “safe harbor” for Certified Persons to disclose Limited Access DMF to other Certified Persons. However, note that any Person, including any Certified Person, who receives Limited Access DMF from a Certified Person, is still subject to penalty under § 1110.200(a)(2), for violations of the Act. The safe harbor provision applies to each disclosure

individually, and only the Certified Person disclosing the information, not the Certified Person recipient, receives the benefit of the presumed compliance with § 1110.102(a)(4)(i)-(iii).

Under § 1110.201 of the final rule, NTIS may conduct, or may request that an Accredited Conformity Assessment Body conduct, at the Certified Person's expense, periodic scheduled and unscheduled audits of the systems, facilities, and procedures of any Certified Person relating to such Certified Person's access to, and use and distribution of, the Limited Access DMF. NTIS contemplates that many, if not most, audits of Certified Persons will be scheduled, but NTIS may also conduct, or request an Accredited Conformity Assessment Body conduct, unscheduled audits—for example, where a prior scheduled audit may have identified the need for adjustment to a Certified Person's systems, facilities, or procedures. Audits conducted by NTIS or by an Accredited Conformity Assessment Body may take place at a Certified Person's place of business (i.e., field audits), or may be conducted remotely (i.e., desk audits). The final rule provides that all Certified Persons be audited with respect to the requirements of § 1110.102(a)(2) no less frequently than every three years under the program, and this requirement may be satisfied by a Certified Person based on an audit or assessment conducted for a purpose other than solely for the purpose of this program. The final rule does not require that Certified Persons undergo routine scheduled audits on the attestation regarding § 1110.102(a)(1), but does provide that unscheduled audits of this and other aspects of the requirements for certification may be conducted at NTIS's discretion. Under the final rule, NTIS' costs for conducting audits will be recoverable from the audited Person. Failure to submit to an audit, to cooperate fully with NTIS in its conduct of an audit or an Accredited Conformity Assessment Body conducting an audit on NTIS’s request, or to pay an audit fee owed to NTIS, are grounds for revocation of certification under the final rule. NTIS intends that a Person or Certified Person will be directly responsible to an Accredited Conformity Assessment Body for any charges by that Accredited Conformity Assessment Body related to requirements under this final rule, as it would be responsible for NTIS' auditing costs under the Act.

Section 1110.200(a)(2) and (b) of the final rule set out the penalties for unauthorized disclosures or uses of the Limited Access DMF. Each individual unauthorized disclosure is punishable by a fine of $1,000, payable to the United States Treasury. However, the total amount of the penalty imposed under this part on any Person for any calendar year shall not exceed $250,000, unless such Person's disclosure or use is determined to be willful or intentional. A disclosure or use is considered willful when it is a "voluntary, intentional violation of a known legal duty." *See U.S. v. Pomponio*, 429 US 10 (1976) (holding that for purposes of interpreting the criminal tax provisions of the Internal Revenue Code, the term "willful" means a voluntary, intentional violation of a known legal duty).

The final rule's § 1110.300 establishes the procedures to appeal a denial or revocation of certification, or the imposition of penalties for violating the Act. An administrative appeal must be filed, in writing, within 30 days (or such longer period as the Director of NTIS may, for good cause shown in writing, establish in any case) after receiving a notice of denial, revocation or imposition of penalties. Appeals are to be directed to the Director of NTIS. Any such appeal must set forth the following: The name, street address, email address and telephone number of the Person seeking review; a copy of the notice of denial or revocation of certification, or the imposition of penalty, from which appeal is taken; a statement of arguments, together with any supporting facts or information, concerning the basis upon which the denial or revocation of certification, or the imposition of penalty, should be reversed; and a request for hearing of oral argument before a representative of the Director, if desired.

Section 1110.300(a)-(d) sets forth the procedures for an administrative appeal. Under § 1110.300(c), a Person may, but need not, retain an attorney to represent such Person in an appeal. A Person must designate an attorney by submitting to the Director of NTIS a written power of attorney. If a hearing is requested, the Person (or the Person's designated attorney) and a representative of NTIS familiar with the notice from which appeal has been taken will present oral arguments which, unless otherwise

ordered before the hearing begins, will be limited to thirty minutes for each side. A Person need not retain an attorney or request an oral hearing to secure full consideration of the facts and the Person's arguments. Where no hearing is requested, the Director shall review the case and issue a decision, as set out below.

Under § 1110.300(e), the Director of NTIS shall issue a decision on the matter within 120 days after a hearing, or, if no hearing was requested, within 90 days of receiving the letter of appeal. In making decisions on appeal, the Director shall consider the arguments and statements of fact and information in the Person's appeal, and made at the oral argument hearing, if such was requested, but the Director at his or her discretion and with due respect for the rights and convenience of the Person and the agency, may call for further statements on specific questions of fact, or may request additional evidence in the form of affidavits on specific facts in dispute. An appellant may seek reconsideration of the decision, but must do so in writing, and the request for reconsideration must be received within 30 days of the Director's decision or within such an extension of time thereof as may be set by the Director of NTIS before the original period expires. A decision shall become final either after the 30-day period for requesting reconsideration expires and no request has been submitted, or on the date of final disposition of a decision on a petition for reconsideration.

Under § 1110.500 of the final rule, an Accredited Conformity Assessment Body must be independent of the Person or Certified Person seeking certification, unless it is a third party conformity assessment body which a Certified Person has qualified for “firewalled” status pursuant to § 1110.502, and must itself be accredited by a recognized accreditation body. The requirement for independence from the Person seeking certification, or from the Certified Person seeking renewal or subject to audit, is important to ensure integrity of any assessment and attestation or audit. The final rule provides that an Accredited Conformity Assessment Body must be an independent third party conformity assessment body that is

not owned, managed, or controlled by a Person or Certified Person that is the subject of attestation or audit by the Accredited Conformity Assessment Body, except where the third party conformity assessment body qualifies for "firewalled" status under § 1110.502.

Accordingly, under the final rule, a Person or Certified Person is considered to own, manage, or control a third party conformity assessment body if the Person or Certified Person holds a 10 percent or greater ownership interest, whether direct or indirect, in the third party conformity assessment body; if the third party conformity assessment body and the Person or Certified Person are owned by a common "parent" entity; if the Person or Certified Person has the ability to appoint a majority of the third party conformity assessment body's senior internal governing body, the ability to appoint the presiding official of the third party conformity assessment body's senior internal governing body, and/or the ability to hire, dismiss, or set the compensation level for third party conformity assessment body personnel; or if the third party conformity assessment body is under a contract to the Person or Certified Person that explicitly limits the services the third party conformity assessment body may perform for other customers and/or explicitly limits which or how many other entities may also be customers of the third party conformity assessment body.

In order for NTIS to accept an attestation as to, or audit of, a Person or Certified Person submitted to NTIS under the final rule, the Accredited Conformity Assessment Body must attest that it is independent of that Person or Certified Person. The Accredited Conformity Assessment Body also must attest that it has read, understood, and agrees to the regulations as set forth in the final rule. The Accredited Conformity Assessment Body must also attest that it is accredited to ISO/IEC Standard 27006-2011 "Information technology—Security techniques—Requirements for bodies providing audit and certification of information security management systems," or to another nationally or internationally recognized standard for bodies providing audit and certification of information security management

systems. The Accredited Conformity Assessment Body must also attest that the scope of its accreditation encompasses the safeguarding and security requirements as set forth in the final rule.

Where review or assessment or audit by an Accredited Conformity Assessment Body was not conducted specifically or solely for the purpose of submission under this part, the final rule requires that the written attestation or assessment report (if an audit) describe the nature of that review or assessment or audit, and that the Accredited Conformity Assessment Body attest that on the basis of such review or assessment or audit, the Person or Certified Person has systems, facilities, and procedures in place to safeguard Limited Access DMF as required under § 1110.102(a)(2).

While NTIS will normally accept written attestations and assessment reports from an Accredited Conformity Assessment Body that attests, to the satisfaction of NTIS, as provided in § 1110.503 of the final rule, the final rule also provides that NTIS may decline to accept written attestations or assessment reports from an Accredited Conformity Assessment Body, whether or not it has attested as provided in § 1110.503, for any of the following reasons: when NTIS determines that doing so is in the public interest under Section 203 of the Bipartisan Budget Act of 2013, and notwithstanding any other provision of these regulations; submission of false or misleading information concerning a material fact(s) in an Accredited Conformity Assessment Body's attestation under § 1110.503; knowing submission of false or misleading information concerning a material fact(s) in an attestation or assessment report by an Accredited Conformity Assessment Body of a Person or Certified Person; failure of an Accredited Conformity Assessment Body to cooperate (as defined in this section) in response to a request from NTIS to verify the accuracy, veracity, and/or completeness of information received in connection with an attestation under § 1110.503 or an attestation or assessment report by that Body of a Person or Certified Person; or where NTIS is unable for any reason to verify the accuracy of the Accredited Conformity Assessment Body's attestation.

In addition, with respect to audits under the final rule, NTIS may in its discretion decline to accept an attestation or assessment report conducted for other purposes, and may conduct or require that an Accredited Conformity Assessment Body conduct a review solely for the purpose of the final rule.

Executive Order 12866

This final rule has been determined to be significant as that term is defined in Executive Order 12866.

Executive Order 13132

A rule has implications for federalism under Executive Order 13132, Federalism, if it has a substantial direct effect on State or local governments and would either preempt State law or impose a substantial direct cost of compliance on States or localities. NTIS has analyzed this rule under that Order and has determined that it does not have implications for federalism.

Final Regulatory Flexibility Analysis

The Regulatory Flexibility Act of 1980, as amended, (RFA), requires agencies to analyze impacts of regulatory actions on small entities (businesses, non-profit organizations, and governments), and to consider alternatives that minimize such impacts while achieving regulatory objectives. Agencies must

first conduct a threshold analysis to determine whether regulatory actions are expected to have significant economic impact on a substantial number of small entities. If the threshold analysis indicates a significant economic impact on a substantial number of small entities, an initial regulatory flexibility analysis must be produced and made available for public review and comment along with the proposed regulatory action. A final regulatory flexibility analysis that considers public comments must then be produced and made publicly available with the final regulatory action.

An Initial Regulatory Flexibility Act Analysis ("IRFA") was incorporated into the NTIS proposed rule. NTIS sought written public comment on the proposed rule, including comment on the IRFA. This Final Regulatory Flexibility Act Analysis ("FRFA") conforms to the RFA, and incorporates the IRFA pursuant to Section 603 and comments received, to analyze the impact that this final rule will have on small entities.

Description of the Reasons Why Action Is Being Considered

The policy reasons for issuing this rule are discussed in the preamble of this document, and not repeated here.

Statement of the Objectives of, and Legal Basis for, the Rule; Identification of All Relevant Federal Rules Which May Duplicate, Overlap, or Conflict with the Rule

The legal basis for this rule is Section 203 of the Bipartisan Budget Act of 2013, Pub. L. 113-67, codified at 42 U.S.C. 1306c (the Act). The rule, which replaces NTIS' interim final rule, implements the Act, which

requires the Secretary of Commerce to create a program to certify that persons given access to the Limited Access DMF satisfy the statutory requirements for accessing that information. Accordingly, this rule creates a permanent program for certifying persons eligible to access Limited Access DMF. It requires that Certified Persons annually re-certify as eligible to access the Limited Access DMF, and that they agree to be subject to scheduled and unscheduled audits. The rule also sets out the penalties for violating the Act's disclosure provisions, establishes a process to appeal penalties or revocations of certification, and adopts a fee program for the certification program, audits, and appeals.

When this final rule becomes effective, it will replace the interim final rule promulgated by NTIS to establish a Temporary Certification Program, in order to avoid the complete loss of access to the Limited Access DMF when the Act became effective. No other rules duplicate, overlap, or conflict with this rule.

Number and Description of Small Entities Regulated by the Action

The final rule applies to all persons seeking to become certified to obtain the Limited Access DMF from NTIS. The entities affected by this rule could include banks and other financial institutions, pension plans, health research institutes or companies, state and local governments, information companies, and similar research services, and others not identified. Many of the impacted entities likely are considered “large” entities under the applicable United States Small Business Administration (SBA) size standards. The SBA defines a “small business” (or “small entity”) as one with annual revenue that meets or is below an established size standard. The SBA “small business” size standard is $550 million in annual revenue for Commercial Banking, Savings Institutions, Credit Unions, and Credit Card Issuing (North American Industry Code (NAICS) 522110, 522120, 522130, and 522210). The size standard is $38.5

million for Consumer Lending and Trust, Fiduciary and Custody Activities, and Direct Health and Medical Insurance Carriers (NAICS 52291, 523991, and 524114), $7.5 million for Mortgage and Nonmortgage Loan Brokers, and Insurance Agencies and Brokerages (NAICS 522310, and 524210), and $32.5 million for Third Party Administration of Insurance and Pension Funds (NAICS 524292). NTIS anticipates that this rule will have an impact on various small entities.

Projected reporting, recordkeeping and other compliance requirements of the rule

Under this final rule, a "Limited Access Death Master File (LADMF) Systems Safeguards Attestation Form" would require Accredited Conformity Assessment Bodies to attest that a Person seeking to be certified to access Limited Access DMF has systems, facilities, and procedures in place as required under § 1110.102(a)(ii) of the rule. NTIS estimates that the type of professional skills necessary for the preparation of an attestation will be those of a senior auditor at an Accredited Conformity Assessment Body, to conduct an assessment under the rule.

Steps NTIS has taken to minimize the significant economic impact on small entities

NTIS carefully considered a number of alternatives to ensure compliance with the safeguarding requirements of Section 203 of the Act. These alternatives included requiring all Persons desiring to become certified to comply with the same requirements as those set forth in Section 6103(p)(4) of the Internal Revenue Code; Section 203(b)(2)(C) of the Act recites that a Certified Person "satisfy the

requirements of such section 6103(p)(4) as if such section applied to such person." Such a requirement would have had a very significant impact on small entities. As pointed out in some comments on the proposed rule, some of the provisions of section 6103(p)(4) would have been extremely burdensome, because, for example, in contrast to Federal Tax Information, Limited Access DMF under Section 203 is not subject to restriction when beyond the three-calendar-year period following the date of death.

Accordingly, NTIS rejected this burdensome alternative, and the final rule instead requires Persons to certify that they have systems, facilities, and procedures in place that are "reasonably similar to" those required by section 6103(p)(4) of the IRC in order to become Certified Persons. This interpretation allows NTIS to meet the interest of protecting personal data generally and deterring fraud, while also allowing NTIS to set the data integrity standards appropriate to safeguard Limited Access DMF specifically, and lessens the burden on small entities which, as noted by a number of commenters, tend not to have in place some more advanced information system controls.

NTIS carefully considered, but rejected, the alternative of requiring Certified Persons to undergo audits annually for the purpose of re-certification. This alternative would have necessitated that a Certified Person bear the expense of assessment for the purpose of attestation by a third party Accredited Conformity Assessment Body each year as part of the annual re-certification process under the rule. Based on consultations with NIST subject matter experts, NTIS concluded instead that a limitation of three years is appropriate as to frequency for assessments for the security and safeguarding of information and information systems, thus lessening the economic impact on small entities under the rule.

NTIS carefully considered, but rejected, the suggestion by a commenter that NTIS itself should accredit third party Accredited Conformity Assessment Bodies. This would have required that NTIS independently develop government-specific accreditation expertise and capacity. Because the Act

requires NTIS to obtain full cost recovery, the cost of such an effort would have to be borne by Certified Persons, including small entities. This would have been inefficient as well as burdensome. Instead, the final rule provides that an Accredited Conformity Assessment Body attest that it is accredited to a nationally or internationally recognized standard for bodies providing audit and certification of information security management systems, and that the scope of its accreditation encompasses the information safeguarding and security requirements as set forth in the rule.

NTIS carefully considered, and rejected, a proposed requirement that Persons desiring to become certified under the rule be limited to program-specific assessments and audits carried out by third party Accredited Conformity Assessment Bodies. This requirement would have necessitated that any Person, including a Person otherwise subject to periodic audit and assessment in the normal course of such Person's business, bear the burden of an additional program-specific audit or assessment for the purposes of the rule. NTIS, however, in consultation with NIST subject matter experts, considered and adopted a less burdensome approach: Provided that a routine assessment or audit of a Person would permit an Accredited Conformity Assessment Body to attest that such Person has systems, facilities, and procedures in place to safeguard Limited Access DMF as required under § 1110.102(a)(2) of the final rule, albeit carried out for a purpose other than certification under the rule, NTIS will accept an attestation in support of a Person's certification with respect to the requirements under § 1110.102(a)(ii) of the rule, as well as in support of the renewal of a Certified Person's certification. Thus, under the final rule, an Accredited Conformity Assessment Body's review or assessment need not have been conducted specifically or solely for the purpose of submission of an attestation under the rule, reducing the economic impact that the rejected alternative would have been imposed on small entities.

NTIS carefully considered, but rejected, the alternative of requiring that a first Certified Person who discloses Limited Access DMF to a second Certified Person be subject to penalty under the rule where,

through no fault of the first Certified Person, the second Certified Person is determined to be subject to penalty under the rule. This alternative would have exposed to penalty under the rule a first Certified Person, who disclosed Limited Access DMF to another Person certified by NTIS, even absent any violation by the first Certified Person. Instead, the Final Rule provides for a “safe harbor” that exempts from penalty a first Certified Person who discloses LADMF to a second Certified Person, where the first Certified Person's liability rests solely on the fact that the second Certified Person has been determined to be subject to penalty. The less burdensome approach chosen by NTIS will reduce the potential economic impact on Certified Persons, including those that are small entities, under such circumstances.

Based on its analysis, NTIS estimates that the rule reflects alternatives placing the least economic impact on small entities, and that the rule will not disproportionately impact small entities as opposed to large ones.

Paperwork Reduction Act

Notwithstanding any other provision of law, no person is required to comply with, and neither shall any person be subject to penalty for failure to comply with, a collection of information subject to the requirements of the Paperwork Reduction Act, unless that collection of information displays a currently valid OMB Control Number.

This final rule contains collection of information requirements subject to review and approval by OMB under the Paperwork Reduction Act (PRA). Approval from OMB will be obtained prior to the final rule becoming effective and prior to the collection of such information, except that NTIS will continue to collect information already approved by OMB under OMB Control No. 0692-0013.

List of Subjects in 15 CFR Part 1110

Administrative appeal, Certification program, Fees, Imposition of penalty.

Dated: May 23, 2016.

Bruce Borzino, Director.

For reasons set forth in the preamble, the National Technical Information Service amends 15 CFR part 1110 as follows:

PART 1110—CERTIFICATION PROGRAM FOR ACCESS TO THE DEATH MASTER FILE

1. The authority for part 1110 continues to read as follows:

Authority: Pub. L. 113-67, Sec. 203.

2. Amend § 1110.2 by:

a. Adding, in alphabetical order, the definition, “Accredited Conformity Assessment Body;” and

b. Revising the definitions of “Limited Access DMF” and “Person”.

The addition and revision read as follows:

§ 1110.2 Definitions used in this part.

* * * * *

Accredited Conformity Assessment Body. A third party conformity assessment body that is accredited by an accreditation body under nationally or internationally recognized criteria such as, but not limited to, International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC)

27006-2011, “Information technology—Security techniques—Requirements for bodies providing audit and certification of information security management systems,” to attest that a Person or Certified Person has systems, facilities and procedures in place to safeguard Limited Access DMF.

* * * * *

Limited Access DMF. The DMF product made available by NTIS which includes DMF with respect to any deceased individual at any time during the three-calendar-year period beginning on the date of the individual's death. As used in this part, Limited Access DMF does not include an individual element of information (name, social security number, date of birth, or date of death) in the possession of a Person, whether or not certified, but obtained by such Person through a source independent of the Limited Access DMF. If a Person obtains, or a third party subsequently provides to such Person, death information (i.e., the name, social security account number, date of birth, or date of death) independently, such information in the possession of such Person is not part of the Limited Access DMF or subject to this part.

* * * * *

Person. Includes corporations, companies, associations, firms, partnerships, societies, joint stock companies, and other private organizations, and state and local government departments and agencies, as well as individuals.

3. Revise the section heading of § 1110.100 to read as follows:

§ 1110.100 Scope; term.

* * * * *

4. Revise § 1110.101 to read as follows:

§ 1110.101 Submission of certification; attestation.

(a) In order to become certified under the certification program established under this part, a Person must submit a completed certification statement and any required documentation, using the most

current version of the Limited Access Death Master File Subscriber Certification Form, and its accompanying instructions at https://dmf.ntis.gov, together with the required fee.

(b) In addition to the requirements under paragraph (a) of this section, in order to become certified, a Person must submit a written attestation from an Accredited Conformity Assessment Body that such Person has systems, facilities, and procedures in place as required under § 1110.102(a)(2). Such attestation must be based on the Accredited Conformity Assessment Body's review or assessment conducted no more than three years prior to the date of submission of the Person's completed certification statement, but such review or assessment need not have been conducted specifically or solely for the purpose of submission under this part.

5. Amend § 1110.102 by revising paragraphs (a)(2), (3), and (4) to read as follows:

§ 1110.102 Certification.

* * * * *

(a) * * *

(2) Such Person has systems, facilities, and procedures in place to safeguard the accessed information, and experience in maintaining the confidentiality, security, and appropriate use of accessed information, pursuant to requirements reasonably similar to the requirements of section 6103(p)(4) of the Internal Revenue Code of 1986;

(3) Such Person agrees to satisfy such similar requirements; and

(4) Such Person shall not, with respect to Limited Access DMF of any deceased individual:

(i) Disclose such deceased individual's Limited Access DMF to any person other than a person who meets the requirements of paragraphs (a)(1) through (3) of this section;

(ii) Disclose such deceased individual's Limited Access DMF to any person who uses the information for any purpose other than a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule, regulation, or fiduciary duty;

(iii) Disclose such deceased individual's Limited Access DMF to any person who further discloses the information to any person other than a person who meets the requirements of paragraphs (a)(1) through (3) of this section; or

(iv) Use any such deceased individual's Limited Access DMF for any purpose other than a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule, regulation, or fiduciary duty.

* * * * *

6. In subpart B of part 1110, add §§ 1110.103, 1110.104, and 1110.105 to read as follows:

§ 1110.103 Disclosure to a certified person.

Disclosure by a Person certified under this part of Limited Access DMF to another Person certified under this part shall be deemed to satisfy the disclosing Person's obligation to ensure compliance with § 1110.102(a)(4)(i) through (iii).

§ 1110.104 Revocation of certification.

False certification as to any element of § 1110.102(a)(1) through (4) shall be grounds for revocation of certification, in addition to any other penalties at law. A Person properly certified who thereafter becomes aware that the Person no longer satisfies one or more elements of § 1110.102(a) shall promptly inform NTIS thereof in writing.

§ 1110.105 Renewal of certification.

(a) A Certified Person may renew its certification status by submitting, on or before the date of expiration of the term of its certification, a completed certification statement in accordance with § 1110.101, together with the required fee, indicating on the form NTIS FM161 that it is a renewal, and also indicating whether or not there has been any change in any basis previously relied upon for certification.

(b) Except as may otherwise be required by NTIS, where a Certified Person seeking certification status renewal has, within a three-year period preceding submission under paragraph (a) of this section, previously submitted a written attestation under § 1110.101(b), or has within such period been subject to a satisfactory audit under § 1110.201, such Certified Person shall so indicate on the form NTIS FM161, and shall not be required to submit a written attestation under § 1110.101(b).

(c) A Certified Person who submits a certification statement, attestation (if required) and fee pursuant to paragraph (a) of this section shall continue in Certified Person status pending notification of renewal or non-renewal from NTIS.

(d) A Person who is a Certified Person before [INSERT DATE 180 DAYS FROM DATE OF PUBLICATION IN FEDERAL REGISTER] shall be considered a Certified Person under this part, and shall continue in Certified Person status until the date which is one year from the date of acceptance of such Person's certification by NTIS under the Temporary Certification Program, provided that if such expiration date falls on a weekend or a federal holiday, the term of certification shall be considered to extend to the next business day.

7. Revise § 1110.200 to read as follows:

§ 1110.200 Imposition of penalty.

(a) *General*. (1) Any Person certified under this part who receives Limited Access DMF, and who:

(i) Discloses Limited Access DMF to any person other than a person who meets the requirements of § 1110.102(a)(1) through (3);

(ii) Discloses Limited Access DMF to any person who uses the Limited Access DMF for any purpose other than a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule, regulation, or fiduciary duty;

(iii) Discloses Limited Access DMF to any person who further discloses the Limited Access DMF to any person other than a person who meets the requirements of § 1110.102(a)(1) through (3); or

(iv) Uses any such Limited Access DMF for any purpose other than a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule, regulation, or fiduciary duty; and

(2) Any Person to whom such Limited Access DMF is disclosed, whether or not such Person is certified under this part, who further discloses or uses such Limited Access DMF as described in paragraphs (a)(1)(i) through (iv) of this section, shall pay to the General Fund of the United States Department of the Treasury a penalty of $1,000 for each such disclosure or use, and, if such Person is certified, shall be subject to having such Person's certification revoked.

(b) *Limitation on penalty*. The total amount of the penalty imposed under this part on any Person for any calendar year shall not exceed $250,000, unless such Person's disclosure or use is determined to be willful or intentional. For the purposes of this part, a disclosure or use is willful when it is a “voluntary, intentional violation of a known legal duty.”

(c) *Disclosure to a Certified Person*. No penalty shall be imposed under paragraphs (a)(1)(i) through (iii) of this section on a first Certified Person who discloses, to a second Certified Person, Limited Access DMF, where the sole basis for imposition of penalty on such first Certified Person is that such second Certified Person has been determined to be subject to penalty under this part.

8. Revise § 1110.201 to read as follows:

§ 1110.201 Audits.

Any Person certified under this part shall, as a condition of certification, agree to be subject to audit by NTIS, or, at the request of NTIS, by an Accredited Conformity Assessment Body, to determine the compliance by such Person with the requirements of this part. NTIS may conduct, or request that an Accredited Conformity Assessment Body conduct, periodic scheduled and unscheduled audits of the systems, facilities, and procedures of any Certified Person relating to such Certified Person's access to, and use and distribution of, the Limited Access DMF. NTIS may conduct, or request that an Accredited Conformity Assessment Body conduct, field audits (during regular business hours) or desk audits of a

Certified Person. Failure of a Certified Person to submit to or cooperate fully with NTIS, or with an Accredited Conformity Assessment Body acting pursuant to this section, in its conduct of an audit, or to pay an audit fee to NTIS, will be grounds for revocation of certification.

Subpart E -- [Redesignated as Subpart E]

9. Redesignate subpart D as subpart E.

10. Add new subpart D to read as follows:

Subpart D – Administrative Appeal

Sec.

1110.3000 Appeal.

Subpart D—Administrative Appeal

§ 1110.300 Appeal.

(a) *General*. Any Person adversely affected or aggrieved by reason of NTIS denying or revoking such Person's certification under this part, or imposing upon such Person under this part a penalty, may obtain review by filing, within 30 days (or such longer period as the Director of NTIS may, for good cause shown in writing, fix in any case) after receiving notice of such denial, revocation or imposition, an administrative appeal to the Director of NTIS.

(b) *Form of appeal*. An appeal shall be submitted in writing to Director, National Technical Information Service, at NTIS's current mailing address as found on its website: www.ntis.gov., ATTENTION DMF APPEAL, and shall include the following:

(1) The name, street address, email address and telephone number of the Person seeking review;

(2) A copy of the notice of denial or revocation of certification, or the imposition of penalty, from which appeal is taken;

(3) A statement of arguments, together with any supporting facts or information, concerning the basis upon which the denial or revocation of certification, or the imposition of penalty, should be reversed;

(4) A request for hearing of oral argument before the Director, if desired.

(c) *Power of attorney*. A Person may, but need not, retain an attorney to represent such Person in an appeal. A Person shall designate any such attorney by submitting to the Director of NTIS a written power of attorney.

(d) *Hearing*. If requested in the appeal, a date will be set for hearing of oral argument before a representative of the Director of NTIS, by the Person or the Person's designated attorney, and a representative of NTIS familiar with the notice from which appeal has been taken. Unless it shall be otherwise ordered before the hearing begins, oral argument will be limited to thirty minutes for each side. A Person need not retain an attorney or request an oral hearing to secure full consideration of the facts and the Person's arguments.

(e) *Decision*. After a hearing on the appeal, if a hearing was requested, the Director of NTIS shall issue a decision on the matter within 120 days, or, if no hearing was requested, within 90 days of receiving the appeal. The decision of the Director of NTIS shall be made after consideration of the arguments and statements of fact and information in the Person's appeal, and the hearing of oral argument if a hearing was requested, but the Director of NTIS at his or her discretion and with due respect for the rights and convenience of the Person and the agency, may call for further statements on specific questions of fact or may request additional evidence in the form of affidavits on specific facts in dispute. After the original decision is issued, an appellant shall have 30 days (or a date as may be set by the Director of NTIS before the original period expires) from the date of the decision to request a reconsideration of the matter. The Director's decision becomes final 30 days after being issued, if no request for reconsideration is filed, or on the date of final disposition of a decision on a petition for reconsideration.

11. Revise newly redesignated subpart E to read as follows:

Subpart E – Fees

Sec.

1110.400 Fees.

Subpart E—Fees

§ 1110.400 Fees.

Fees sufficient to cover (but not to exceed) all costs to NTIS associated with evaluating Certification Forms and auditing, inspecting, and monitoring certified persons under the certification program established under this part, as well as appeals, will be published (as periodically reevaluated and updated by NTIS) and available at https://dmf.ntis.gov. NTIS will not set fees for attestations or audits by an Accredited Conformity Assessment Body.

12. Add subpart F to read as follows:

Subpart F – Accredited Conformity Assessment Bodies

Sec.

1110.500 Accredited conformity assessment bodies.

1110.501 Independent.

1110.502 Firewalled.

1110.503 Attestation by accredited conformity assessment body.

1110.504 Acceptance of accredited conformity assessment bodies.

Subpart F—Accredited Conformity Assessment Bodies

§ 1110.500 Accredited conformity assessment bodies.

This subpart describes Accredited Conformity Assessment Bodies and their accreditation for third party attestation and auditing of the information safeguarding requirement for certification of Persons under this part. NTIS will accept an attestation or audit of a Person or Certified Person from an Accredited Conformity Assessment Body that is:

(a) Independent of that Person or Certified Person; or

(b) Is firewalled from that Person or Certified Person, and that in either instance is itself accredited by a nationally or internationally recognized accreditation body.

§ 1110.501 Independent.

(a) An Accredited Conformity Assessment Body that is an independent third party conformity assessment body is one that is not owned, managed, or controlled by a Person or Certified Person that is the subject of attestation or audit by the Accredited Conformity Assessment Body.

(1) A Person or Certified Person is considered to own, manage, or control a third party conformity assessment body if any one of the following characteristics applies:

(i) The Person or Certified Person holds a 10 percent or greater ownership interest, whether direct or indirect, in the third party conformity assessment body. Indirect ownership interest is calculated by successive multiplication of the ownership percentages for each link in the ownership chain;

(ii) The third party conformity assessment body and the Person or Certified Person are owned by a common “parent” entity;

(iii) The Person or Certified Person has the ability to appoint a majority of the third party conformity assessment body's senior internal governing body (such as, but not limited to, a board of directors), the ability to appoint the presiding official (such as, but not limited to, the chair or president) of the third party conformity assessment body's senior internal governing body, and/or the ability to hire, dismiss, or set the compensation level for third party conformity assessment body personnel; or

(iv) The third party conformity assessment body is under a contract to the Person or Certified Person that explicitly limits the services the third party conformity assessment body may perform for other customers and/or explicitly limits which or how many other entities may also be customers of the third party conformity assessment body.

(2) A state or local government office of Inspector General or Auditor General and a Person or Certified Person that is a department or agency of the same state or local government, respectively, are not considered to be owned by a common "parent" entity under paragraph (a)(1)(ii) of this section.

(b) [Reserved]

§ 1110.502 Firewalled.

(a) A third party conformity assessment body must apply to NTIS for firewalled status if it is owned, managed, or controlled by a Person or Certified Person that is the subject of attestation or audit by the Accredited Conformity Assessment Body, applying the characteristics set forth under § 1110.501(a)(1).

(b) The application for firewalled status of a third party conformity assessment body under paragraph (a) of this section will be accepted by NTIS where NTIS finds that:

(1) Acceptance of the third party conformity assessment body for firewalled status would provide equal or greater assurance that the Person or Certified Person has information security systems, facilities, and procedures in place to protect the security of the Limited Access DMF than would the Person's or Certified Person's use of an independent third party third party conformity assessment body; and

(2) The third party conformity assessment body has established procedures to ensure that:

(i) Its attestations and audits are protected from undue influence by the Person or Certified Person that is the subject of attestation or audit by the Accredited Conformity Assessment Body, or by any other interested party;

(ii) NTIS is notified promptly of any attempt by the Person or Certified Person that is the subject of attestation or audit by the third party conformity assessment body, or by any other interested party, to hide or exert undue influence over an attestation, assessment or audit; and

(iii) Allegations of undue influence may be reported confidentially to NTIS. To the extent permitted by Federal law, NTIS will undertake to protect the confidentiality of witnesses reporting allegations of undue influence.

(c) NTIS will review each application and may contact the third party conformity assessment body with questions or to request submission of missing information, and will communicate its decision on each application in writing to the applicant, which may be by electronic mail.

§ 1110.503 Attestation by accredited conformity assessment body.

(a) In any attestation or audit of a Person or Certified Person that will be submitted to NTIS under this part, an Accredited Conformity Assessment Body must attest that it is independent of that Person or Certified Person. The Accredited Conformity Assessment Body also must attest that it has read, understood, and agrees to the regulations in this part. The Accredited Conformity Assessment Body must also attest that it is accredited to a nationally or internationally recognized standard such as the ISO/IEC Standard 27006-2011 “Information technology—Security techniques—Requirements for bodies providing audit and certification of information security management systems,” or any other similar nationally or internationally recognized standard for bodies providing audit and certification of information security management systems. The Accredited Conformity Assessment Body must also attest that the scope of its accreditation encompasses the safeguarding and security requirements as set forth in this part.

(b) Where a Person seeks certification, or where a Certified Person seeks renewal of certification or is audited under this part, an Accredited Conformity Assessment Body may provide written attestation that such Person or Certified Person has systems, facilities, and procedures in place as required under § 1110.102(a)(2). Such attestation must be based on the Accredited Conformity Assessment Body's review or assessment conducted no more than three years prior to the date of submission of the Person's or Certified Person's completed certification statement, and, if an audit of a Certified Person by an Accredited Conformity Assessment Body is required by NTIS, no more than three years prior to the date upon which NTIS notifies the Certified Person of NTIS's requirement for audit, but such review or

assessment or audit need not have been conducted specifically or solely for the purpose of submission under this part.

(c) Where review or assessment or audit by an Accredited Conformity Assessment Body was not conducted specifically or solely for the purpose of submission under this part, the written attestation or assessment report (if an audit) shall describe the nature of that review or assessment or audit, and the Accredited Conformity Assessment Body shall attest that on the basis of such review or assessment or audit, the Person or Certified Person has systems, facilities, and procedures in place as required under § 1110.102(a)(2).

(d) Notwithstanding paragraphs (a) through (c) of this section, NTIS may, in its sole discretion, require that review or assessment or audit by an Accredited Conformity Assessment Body be conducted specifically or solely for the purpose of submission under this part.

§ 1110.504 Acceptance of accredited conformity assessment bodies.

(a) NTIS will accept written attestations and assessment reports from an Accredited Conformity Assessment Body that attests, to the satisfaction of NTIS, as provided in § 1110.503.

(b) NTIS may decline to accept written attestations or assessment reports from an Accredited Conformity Assessment Body, whether or not it has attested as provided in § 1110.503, for any of the following reasons:

(1) When it is in the public interest under Section 203 of the Bipartisan Budget Act of 2013, and notwithstanding any other provision of this part;

(2) Submission of false or misleading information concerning a material fact(s) in an Accredited Conformity Assessment Body's attestation under § 1110.503;

(3) Knowing submission of false or misleading information concerning a material fact(s) in an attestation or assessment report by an Accredited Conformity Assessment Body of a Person or Certified Person;

(4) Failure of an Accredited Conformity Assessment Body to cooperate in response to a request from NTIS to verify the accuracy, veracity, and/or completeness of information received in connection with an attestation under § 1110.503 or an attestation or assessment report by that Body of a Person or Certified Person. An Accredited Conformity Assessment Body “fails to cooperate” when it does not respond to NTIS inquiries or requests, or it responds in a manner that is unresponsive, evasive, deceptive, or substantially incomplete; or

(5) Where NTIS is unable for any reason to verify the accuracy of the Accredited Conformity Assessment Body's attestation.

[FR Doc. 2016-12479 Filed: 5/31/2016 8:45 am; Publication Date: 6/1/2016]